



Digital Security & U.S. Political Campaigns: Research Highlights

Note: These are early results which may evolve and be expanded as we continue analysis. This work is part of a broader effort of studying the attitudes, practices, and challenges of users who may be at higher risk of targeted digital attacks because of who they are with, what they do, where they are, or who they are. Past research of ours in this space has included studies of survivors of intimate partner abuse, women in South Asia, and people who are struggling financially.

Digital Security & U.S. Political Campaigns: Research Highlights

“What is 100% true... is that foreign adversaries want <campaign> information... The faster we all realize that, the better off we’re going to be... to see politics and campaigns at all levels as a fundamental piece of democracy that needs to be protected.... For sure foreign adversaries are trying to attack our systems... Why wouldn’t someone think of democracy as a target?” –A study participant

Democratic institutions related to political campaigns and elections are at risk of digital security attacks. We have conducted research to understand the digital security practices, challenges, and perceptions of people involved in politics, with a focus on U.S. campaigns across the political spectrum. Our goal with this user-focused research is to help improve technology and to provide digital security education to political campaigns and those who support them. Improving the digital security of campaigns is a non-partisan issue that is an important part of preserving democratic institutions.

The Study

As part of an ongoing series of research studying high-risk users, we conducted a qualitative interview study with 25+ people who have experience working with or supporting U.S. political campaigns across the political spectrum in 2019-2020. Many of the participants had several years of experience and had served in multiple campaign-related roles (including as candidates, elected officials, campaign managers, chiefs of staff, digital directors, research or strategy, and security or IT staff) across a range of organizations (including campaigns, political offices, party committees, super PACs, campaign-specific services, and academia). Large and small campaigns (from presidential, senate, and gubernatorial to small congressional and local races) were represented. Interviews were semi-structured. Most were conducted in person with one participant at a time, ranging from 40 to 120 minutes each in length (average of 72 minutes). To analyze the data, interviews were audio recorded, transcribed, and analyzed for themes.

As with any interview study, this research is subject to the typical limitations of recall and observer bias. Also, the sample is small, so the results do not represent all political workers or campaigns. Instead, we aimed to understand a small sample of experiences in depth. As with all studies of security and privacy, our focus on digital security and privacy during the interviews may have biased results (e.g., by causing an over-indexing on concerns). Finally, from what we understand, the landscape of digital security for U.S. political campaigns has been rapidly evolving since the well-known hacks of 2015 and 2016. Further, the COVID-19 global pandemic is likely adding to this evolution with increased virtual work and other strategies. As such, we attempted to focus on participants who had experience on or with campaigns since the 2016 hacks; we expect the field will continue to evolve.

What We Learned

In what follows, we provide a broad overview of political campaigns' digital security practices and the main security attacks and attackers campaigns believe they face. Then we describe themes that pertain to digital security and abuse risks for campaigns: digital communications, account security, 2-factor authentication, and information campaigns. All of the quotes that follow are from participants, as they describe their experiences and opinions.

Political Campaign Security Culture

According to our interviews, the primary goal of a campaign is to win the election. Any activities that are viewed as not directly in support of this goal are deprioritized—and this often includes preventative security measures. Campaigns were described as chaotic and temporary, ramped up much like an early-stage start-up, but without the time for any permanent infrastructure—like hardened security infrastructure and policies. Election Day in November is a firm deadline that doesn't move or slip, while all funds must be raised as the campaign progresses, causing a sense of rushed, ruthless prioritization regarding how campaign workers spend their time and effort.

"So I think one challenge you have with campaigns is they're totally transient, and almost everybody gets hired in the 3 months prior to the election. So that's the first problem you have with campaigns. Totally transient, and there's really no — very few incentives for any kind of <security> rigor. Period. Because you're up against the clock, and faced with the ticking clock, everything pales." —A study participant

The hacks of 2015 and 2016 were a tipping point for security attitudes among campaign workers. Several political campaign and committee workers' accounts were compromised and data was leaked to the public. Awareness of security risks, and in some cases behaviors, changed as a result. But these changes are in the early stages, and digital security remains "an afterthought" to many campaign workers, according to our participants.

"...my experience with political campaigns is they were broadly ignorant / negligent at pretty much all security measures until <the 2016 hack>. And then, suddenly, everybody got worried." –A study participant

"<Politician has this saying about campaigns>, 'There's the wolf in your yard, there's the wolf on your deck, there's the wolf in your house, and there's the wolf in your pants.' Cybersecurity is like the wolf in your yard. You can't even get there because you have these day-to-day things that consume your life. It's very difficult to look past that wolf in your pants... You're on these tight deadlines..." –A study participant

Attacks and Attackers

Participants reported that political campaigns face various attacks aimed to influence elections, candidates, and generally create chaos and discord. Phishing was their top concern; it was described as being cheap, easy, capable of causing considerable damage, and it worked in 2016. Other concerns included information campaigns (mis/disinformation and fake news), skilled attacks (like malware and DDoS), social engineering, accidental sharing, harassment, physical compromise, and violence.

[Phishing] "It makes logical sense that, low-cost, high-volume, remote attacks are happening all the time. Especially when we saw them successful in 2016. How many pennies did it cost to phish <campaign staffer>, and what was the return on that investment?... When you're working with a Congressional campaign, someone might say, 'This security stuff sounds like a hassle. Why would anyone care about me anyway? I'm just one person running for Congress...' And to sort of get your head around that, the marginal cost of attacking all campaigns, as opposed to just one campaign, is minuscule. You just need to gather the email addresses. Computer power's free, essentially. Emailing is free, essentially. Phishing, if you've... designed a good phishing campaign and set up the site to receive credentials, whether you send a lure to 1 person or 10,000 people is a marginal cost of pennies. So why would you bother attacking just one campaign and not all of them?" –A study participant

[Accidental sharing] "[Do lower-level staff understand they're targets?] I think you have to continue to remind them. I also think they grew up in a different environment where sharing is just what they do... They also probably don't think they're vulnerable because, why would anyone care what they think? But they're an entry point because they have access to the server, they have access to all that information, so it's an ongoing process to remind them." –A study participant

[Harassment] "The only remedy that we would have to get that <social media post> off is an outright block, which... elected officials can't block people anymore." –A study participant

Regarding potential attackers, participants expressed the most concern about nation-state attackers. Some expressed concern about citizens, citizen groups, or special interest groups. There was less (but not no) concern about the other political party, their own party, insiders, or journalists. Regardless of the

attacker, participants were concerned about information being leaked to all of the above, voters, and others as a result of an attack.

[Nation-states] “There were no repercussions from the last time <a nation-state interfered in the 2016 election>... We tried to have sanctions, the sanctions were lifted. There’s no reason why they wouldn’t attempt to do it again... And I think that on top of that, other foreign governments realized how successful that was for <a nation-state>, and it would not be surprising if we saw an increase in <another nation-state> interference or other foreign governments as well, considering how easy it was for the <nation-state>. And I say easy as in ROI—like the amount of effort, money they had to spend in order to affect change and influence the campaigns was barely negligible on a grand scale—especially for a nation-state.” –A study participant

[Not opponents] “...ever since I’ve worked here, <we> have been worried about a foreign entity hacking us... I’ve never worried about <the other party> hacking us. I just don’t—maybe it’s because we’ve never been like that, so I assume they’re not.” –A study participant

Digital Communications

When asked about what information they were most worried about being stolen or leaked, participants primarily talked about digital communications. Communications to or from people involved with political campaigns were considered sensitive. If leaked, potentially any communications could cause serious damage to the campaign. Participants believed that, as a result, communications were a big focus of attackers—and some thought they were the primary focus, due to the extent of damage they can cause to a campaign or candidate. Security practices for communications accounts create vulnerabilities (as described further in the next section). To mitigate, participants noted increased use of end-to-end encrypted messaging systems and (to a lesser extent) deletion policies and practices.

[Nation-states target comms] “[What are nation-states after?] Emails, communications, anything that could compromise the campaign, make it look bad. I think the data as well. But what they went after last time was any communications. Like they went after the <committee> – what <committee members> were saying internally, that could be used against them in press and in public... Anything that makes the campaign or the staff look bad... I think <communications are> probably more important, frankly, than the data.” –A study participant

[Leaked comms cause damage] “Let’s say the candidate is just <complaining> about something. Or staff is just <complaining> about something. Someone could very easily grab that and turn it into a thing, when it was actually just a ‘human moment,’ and now you’ve derailed the whole campaign. You’ve taken it off message. You’re talking about whatever stupid, petty thing was in that email, as opposed to equal pay, or fixing transportation, or whatever you really want to be talking about.” –A study participant

[Encrypted messaging] “[What content is most important to secure?] It’s basically communications and social media. So start with communications, and that’s account and personal. So that’s primarily email... and encouraging people to move to secure communications tools like <e2e chat>, instead of SMS. [Do they use encrypted chat tools?] I think that one is mostly successful because that fits in the right category, where those tools are high quality, the user experience is good, and it’s something that makes people feel like they’re doing something. And it’s visible... As opposed to a lot of the security practices you have to put in place that feel like a pain in the ass for something that might not even happen, and you don’t see anything visible.” – A study participant

Account Security

Campaign workers use a plethora of personal accounts for campaign information and communications, even when workplace systems (like G Suite or Office 365) are used. IT staff (if the campaign employs any) are unable to protect or control personal accounts of the many people working on the campaign. Some campaign-related accounts are *hyper-shared* and/or *hyper-owned*—that is, many workers may need to access them, and account ownership may change from cycle to cycle—making it hard to use some security features. Together, these practices leave communications and other information stored in campaign workers’ accounts vulnerable to security attacks.

[Personal accounts] “...largely what ends up happening is what I’ll call ‘work product’ ends up in their personal accounts. So you go after the personal accounts, they have been shared on polling, on digital trends, plans, what emails we’re going to send out... that sort of stuff. All this is being shared in <cloud-based docs> to their personal account that <IT staff> can’t secure... I’m fine with you using <chat app>. Don’t share the corporate secrets there. Don’t share confidential information there, because it will largely be hacked and targeted by nation-states as it already has been.” –A study participant

[Hyper-owned accounts] “...that’s the other thing: 2-step verification... it’s always or often like someone’s phone number who no longer works for the campaign. And to update which phone is associated with each account—that’s really important...” –A study participant

2-Factor Authentication

Many participants considered 2-factor authentication (2FA) the most important security measure for people working on or supporting campaigns to use, since phishing was a major attack, account security was a main vulnerability, and the communications stored in certain accounts could be highly sensitive. Given their experiences with campaigns, participants believed that most campaign workers have likely heard of 2FA, use some form of it on at least one account, and associate it with being an important part of account security. However, 2FA is under-utilized across campaign workers’ many accounts and they often use weaker second factors (such as SMS codes). We inferred from participants that most people on or involved with campaigns did not understand how 2FA improves their security, that different types of

second factors offer different levels of protection, and that they should use 2FA to protect most of their accounts (or they were aware, but had not acted upon it).

[2FA on some accounts] “[Do you have 2FA on most accounts?] Not all of them, but some of them. [How do you decide which accounts?] Mostly, what I’m prompted for, what is more called to my attention.” –A study participant

[Limited understanding] “[What attacks might the code via phone call be vulnerable to?] I don’t know... I have no idea. [How about the app?] It just seems really complicated to set up. But hacking I guess? I don’t know.” –A study participant

Participants described several pain points of 2FA, including the extra time and effort they perceived that it takes to set up and use (especially for hyper-shared, hyper-owned, and personal accounts), and concern about being locked out of an account sometime in the future—or worse, if the candidate or a senior staff member were to get locked out of an account.

[Phone-based 2FA issues] “Well, what happens if your phone is dead?... You’re screwed... <My phone is> dead a lot... You know, I’m on the road... I think the 2-factor, that’s pretty annoying if your phone died.” –A study participant

[Security key issues] “Except I’d lose a fob. I’m always losing those things... Like my phone is always there. So that’s why I like the phone—either the thing that calls or a text message, because <the phone is> an appendage.” –A study participant

Information Campaigns

Participants believe that information campaigns (e.g., mis/disinformation, fake news) are eroding democracy by sowing discord and chaos, and dismantling a shared sense of what is true among Americans. They posited that nation-states, unwitting users, and profiteers leverage and exploit online platforms to advance information campaigns to unprecedented scale. Participants agreed with each other that this is an extremely challenging problem, and that solutions are not obvious. Some called for regulation, some argued that tech companies should be responsible, and many thought government and tech companies should work together—and quickly—to solve this growing problem for democracy.

[Impact on democracy] “<Fake news is> sowing discord into democracy, because democracy requires and relies on people being educated, participating, compromising, protecting the Constitution, working together, having shared values. Democracy relies on that. It’s an idea. And so if you can chip away at those pieces of it, you know, the hope is that the whole thing crumbles and then if democracy’s not strong, anti-democratic countries do better in the world order.” –A study participant

[Disinfo hard to prevent] “And the other <major attack> is disinformation, which is a much harder thing to wrap your head around and/or control. So I can secure my website, I can secure my email, I can secure my network and educate my users so we don’t get compromised, but that still does nothing against disinformation campaigns online about <social media company> trolls, <other social media company>, stuff like that.” –A study participant

[Call for regulation] “I think fake news should be regulated. Somehow. [Who decides?] Ideally you’d have the powers that be within our democratic institution, which includes the courts, and Congress, and government regulators, to put not the answer, but the guardrails, and the direction, and the protections on the system... That’s not corporate’s role. The number one priority of corporations is to make money. And it’s a secondary goal to protect people and do the right thing... But the primary role of government is to protect people... Which is why they should be the ones determining, because they are the ones that, in theory, have the people’s interest in mind.” –A study participant

[Call for standards] “We need to have a better business bureau for content. [Who should be making these decisions?] I don’t know. But I’m telling you, democracy depends on it. If we had a <foundation> that everybody could agree was the gold standard of determining, not necessarily unbiased but certainly reliable, print a retraction when they’re wrong, kind of information. That’s one thing... You have to have some level of reliability and authenticity...” –A study participant

Summary

We conducted a qualitative interview study to understand the digital security practices, challenges, and perceptions of people involved in U.S. campaigns across the political spectrum (with 25+ people who have experience working with or supporting U.S. political campaigns). We found that campaigns have not fully adapted to the various digital security attacks that they face today. Phishing and information campaigns were top concerns, particularly by nation-state actors. Communications of campaign workers, if leaked, could cause serious damage to their campaign (or party). These communications were housed in a plethora of campaign and personal accounts that have been targeted by attackers. At the same time, it appears that campaign workers under-used 2FA on their accounts, often used weaker second factors, and had limited understanding of 2FA. To mitigate these issues, we intend to use the results of this study to help improve digital security technology and education for campaign workers.